

# EXHIBIT 1

COPY

FILED IN CHAMBERS

FEB 13 2015

U.S. MAGISTRATE JUDGE  
N.D. GEORGIA

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
E-MAIL ADDRESSES

jshaw405@gmail.com,  
411webmarketing@gmail.com,  
terry.tcbgroup@gmail.com,  
thegetteammanagers@gmail.com,  
rrhame@gmail.com and  
SCGCompliance@gmail.com THAT IS  
STORED AT PREMISES CONTROLLED BY  
GOOGLE, INC., AN EMAIL PROVIDER  
HEADQUARTERED AT 1600  
AMPHITHEATER PKWY, MOUNTAIN  
VIEW, CA 94043

Criminal Action No.

1:15-MC-110

UNDER SEAL

**NON-DISCLOSURE AND SEALING ORDER**

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding the Service Provider to whom the attached search warrant is addressed ("Service Provider"), an electronic communications service provider and/or a remote computing service, not to notify any person (including the subscribers or customers of the account/s listed in the attached search warrant) of the existence of the search warrant until further order of the Court. The United States also moves to seal the

search warrant, the application and affidavit pertaining to such warrant, this application, any attachments thereto, and this Order.

The Court finds that there is reason to believe that notification as to the existence of the search warrant in this matter will seriously jeopardize an ongoing investigation, potentially by giving the target/s: (a) an opportunity to flee or continue flight from prosecution, (b) destroy or tamper with evidence, (c) change patterns of behavior, and (d) notify confederates. See 18 U.S.C. § 2705(b)(2)-(3), (5). For the same reasons, the Court finds that there is good cause to seal the search warrant, the application and affidavit pertaining to such warrant, this application, any attachments thereto, and this Order.


IT IS HEREBY ORDERED, under 18 U.S.C. § 2705(b), that the Service Provider shall not disclose the existence of the search warrant or this Order, to the listed subscribers/customers or to any other person: (a) unless and until the investigation is completed, or (b) unless otherwise authorized to do so by the Court.

IT IS FURTHER ORDERED that the Service Provider may disclose the search warrant to its attorney for the purpose of receiving legal advice. Furthermore, at any time, the Service Provider may inquire about the status of the investigation by contacting the Assistant United States Attorney listed on the

search warrant and below, or may seek authorization to disclose by filing a motion under seal with this Court and serving a copy of said motion on the listed Assistant United States Attorney.

IT IS FURTHER ORDERED that the search warrant, the application and affidavit pertaining to such warrant, this application, any attachments thereto, and this Order, be SEALED until further order of the Court.

SO ORDERED, this 13<sup>th</sup> day of February, 2015.

  
GERRILYN G. BRILL  
UNITED STATES MAGISTRATE JUDGE

Prepared by:  
Thomas J. Krepp, AUSA  
United States Attorney's Office  
600 U.S. Courthouse  
75 Spring St., S.W.  
Atlanta, GA 30303  
(404)581-4647  
(404)581-6181 (Fax)

CONFIDENTIAL

FILED IN CHAMBERS

FEB 13 2015

U.S. MAGISTRATE JUDGE  
N.D. GEORGIA

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
E-MAIL ADDRESSES

jshaw405@gmail.com,  
411webmarketing@gmail.com,  
terry.tcbgroup@gmail.com,  
thegetteammanagers@gmail.com,  
rrhame@gmail.com and  
SCGCompliance@gmail.com THAT IS  
STORED AT PREMISES CONTROLLED BY  
GOOGLE, INC., AN EMAIL PROVIDER  
HEADQUARTERED AT 1600  
AMPHITHEATER PKWY, MOUNTAIN  
VIEW, CA 94043

Criminal Action No.

1:15-MC-110

**UNDER SEAL**

**APPLICATION FOR ORDER COMMANDING GOOGLE, INC. NOT TO  
NOTIFY ANY PERSON OF THE EXISTENCE OF A SEARCH WARRANT  
AND MOTION TO SEAL**

The United States of America, by John A. Horn, Acting United States Attorney for the Northern District of Georgia, and Thomas J. Krepp Assistant United States Attorney, requests: (a) that the Court prohibit Google, Inc. (the "Service Provider") from disclosing the existence of the search warrant issued in the above captioned matter, and (b) that the Court seal the search warrant, the

In support of its petition, the United States submits as follows:

1. The Service Provider is a provider of an “electronic communication service,” as defined in 18 U.S.C. § 2510(15) and/or is a provider of “remote computing service,” as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, the United States will serve the search warrant issued in this matter on the Service Provider, requiring the Service Provider to produce certain records and information to the United States described in such warrant.

2. Under 18 U.S.C. § 2705(b), federal courts have the authority to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.”

3. In this case, the search warrant relates to an ongoing criminal investigation that is neither public nor known to some of the targets of the investigation. See ACLU v. Holder, 673 F.3d 245, 253 (4th Cir. 2011) (“[t]he United States has a compelling interest in protecting the integrity of ongoing ... investigations”). As a result, the United States submits that disclosing the existence of the search warrant could seriously jeopardize the instant investigation, by giving the target/s an opportunity: (a) to flee or continue flight

from prosecution, (b) to destroy or tamper with evidence, (c) to alter behavior patterns, and (d) to notify confederates. See 18 U.S.C. §§ 2705(b)(2)-(3), (5).

4. Based on the same reasons set forth above, the United States also requests that the search warrant, the application and affidavit pertaining to such warrant, this application, any attachments thereto, and any corresponding order be sealed until further order of this Court. See United States v. Gomez, 323 F.3d 1305, 1307 (11th Cir. 2003) (“district courts have substantial supervisory powers over their records and files”).

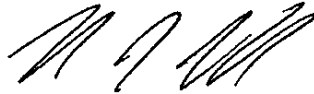
WHEREFORE, the United States respectfully requests that the Court order the Service Provider not to disclose the existence or content of the search warrant (except that the Service Provider may disclose the search warrant to the Service Providers’ attorneys for the purpose of receiving legal advice). The United States also requests that the search warrant, the application and affidavit pertaining to such warrant, this application, any attachments thereto, and any corresponding order, be sealed until further order of this Court.

Dated: February 13, 2015

Respectfully submitted,

JOHN A. HORN

*Acting United States Attorney*



THOMAS J. KREPP

Assistant United States Attorney

75 Spring Street, SW, Suite 600

Atlanta, GA 30303

404.581.4647

Georgia Bar No. 346781



COF

(Rev. 4/30/2014) Search Warrant

United States District Court

Northern District of Georgia

In the Matter of the Search of:

Information associated with the email addresses  
jshaw405@gmail.com, 411webmarketing@gmail.com,  
terry.tcbgroup@gmail.com,  
thegetteammanagers@gmail.com, rrhame@gmail.com and  
SCGCompliance@gmail.com that is stored at premises  
owned, maintained, controlled, or operated by Google, Inc.,  
an email provider headquartered at 1600 Amphitheater  
Pkwy, Mountain View, CA 94043

SEARCH WARRANT

CASE NUMBER: 1:15-MC-110

UNDER SEAL

TO: FBI Special Agent W. Scott Baucom and any Authorized Officer of the United States:

An affidavit having been made before me by Special Agent W. Scott Baucom, who has reason to believe that, on the property or  
premises known as

See Attachment A

There is now concealed certain property, certain data, and certain information, namely,

See Attachment B

which constitutes evidence of the commission of a criminal offense and property which has been used as the means of committing a  
criminal offense, concerning violations of Title 18, United States Code, Sections 1343 and 1956, over which the United States District  
Court for the Northern District of Georgia has jurisdiction. I find that the affidavit establishes probable cause to search and seize the  
person or property from the person or premises described above.

YOU ARE HEREBY COMMANDED to execute this warrant on or before 2/27/15  
Date

(not to exceed 14 days) AT ANY TIME IN THE DAY OR NIGHT AS I FIND GOOD CAUSE HAS BEEN ESTABLISHED. You must  
give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was  
taken, or leave a copy of the warrant and receipt at the place where the property was taken. The officer executing the warrant, or an  
officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant  
and inventory to United States Magistrate Judge Gerrilyn G. Brill

February 13, 2015 at 1:55 PM  
Date and Time

at Atlanta, Georgia  
City and State

GERRILYN G. BRILL  
UNITED STATES MAGISTRATE JUDGE  
Name and Title of Judicial Officer

Gerrilyn Brill  
Signature of Judicial Officer

AUSA Thomas J. Krepp /404-581- 4647

SW-000157

**ATTACHMENT A**

**Property to Be Searched**

1. This warrant applies to information associated with the email addresses **jshaw405@gmail.com, rrhame@gmail.com, terry.tcbgroup@gmail.com, thegetteammanagers@gmail.com, SCGCompliance@gmail.com, and 411webmarketing@gmail.com** which are stored at premises owned, maintained, controlled, or operated by Google, Inc., an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

A. The contents of all emails stored in the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

B. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

C. All records pertaining to communications between Google, Inc. and any person regarding the account, including contacts with support services and records of actions taken.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 1343 and 1956 and conspiracy to commit these

offenses, including for each account or identifier listed on Attachment A, information pertaining to the following matters:

- A. The identity of the person(s) who created, used, or communicated with the account or identifier, including records that help reveal the whereabouts of such person(s).
- B. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events.
- C. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation.
- D. Records relating to buying and selling of currency, commodities, and securities.
- E. Records related to the users' financial information, including but not limited to bank accounts, tax information, additional sources of income or revenue, expenditures, and the disposition of proceeds.
- F. Records relating to Sterling Currency Group / DinarBanker, including but not limited to the corporate structure, correspondence with Sterling employees, payments from Sterling, direction from Sterling employees, and corporate documents.
- G. Records relating to websites that discuss currency sales or exchanges, including but not limited to, registration and maintenance of the websites, statements on the websites, and payment information.
- H. Records related to the advertisement of Sterling Currency Group / DinarBanker.
- I. Records related to the users' involvement with web development, web design, and blog registration or maintenance.

COPY

(Rev. 4/30/2014 Search Warrant)

FILED IN CHAMBERS

## United States District Court

Northern District of Georgia

FEB 13 2015  
U.S. MAGISTRATE JUDGE  
N.D. GEORGIA

In the Matter of the Search of:

Information associated with the email addresses  
 jshaw405@gmail.com, 411webmarketing@gmail.com,  
 terry.tcbgroup@gmail.com,  
 thegetteammanagers@gmail.com, rrhame@gmail.com and  
 SCGCompliance@gmail.com that is stored at premises  
 owned, maintained, controlled, or operated by Google, Inc.,  
 an email provider headquartered at 1600 Amphitheater  
 Pkwy, Mountain View, CA 94043

APPLICATION & AFFIDAVIT  
FOR SEARCH WARRANT

CASE NUMBER: 1:15-MC-110

UNDER SEAL

I, W. Scott Baucom, being duly sworn, depose and says:

I am a(n) Special Agent of the FBI, and have reason to believe that, on the property or premises known as

See Attachment A

There is now concealed certain property, certain data, and certain information, namely,

See Attachment B

which constitutes evidence of the commission of a criminal offense and property which has been used as the means of committing a criminal offense, concerning violations of Title 18, United States Code, Sections 1343 and 1956, over which the United States District Court for the Northern District of Georgia has jurisdiction. The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof.

☒ Yes ☐ No

W. Scott Baucom

Signature of Affiant

W. Scott Baucom

Sworn to before me, and subscribed in my presence

February 13, 2015

Date

at Atlanta, Georgia

City and State

GERRILYN G. BRILL

UNITED STATES MAGISTRATE JUDGE

Name and Title of Judicial Officer

Gerrilyn Brill

Signature of Judicial Officer

AUSA Thomas J. Krepp /404-581- 4647

SW-000161

**AFFIDAVIT**

I, W. Scott Baucom, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for search warrants for information associated with:

- A. the Microsoft Corporation ("Microsoft") email address **twshawdc@hotmail.com** which is stored at premises owned, maintained, controlled, or operated by Microsoft, an email provider headquartered at One Microsoft Way, Redmond, Washington 98052;
- B. the AOL, Inc. ("AOL") email addresses **tcbgroupinc@aol.com**, **jimmendez320@aol.com** and **lauretteshaw@aol.com** which are stored at premises owned, maintained, controlled, or operated by AOL, an email provider headquartered at 22000 AOL Way, Dulles, Virginia 20166;
- C. the Google, Inc. ("Google") email addresses **jshaw405@gmail.com**, **rrhame@gmail.com**, **terry.tcbgroup@gmail.com**, **thegetteammanagers@gmail.com**, **SCGCompliance@gmail.com**, and **411webmarketing@gmail.com** which are stored at premises owned, maintained, controlled, or operated by Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043;
- D. The Yahoo! Inc. ("Yahoo!") email addresses **dansilverman@yahoo.com** and **hectorperezpr@yahoo.com**, which are stored at premises owned, maintained, controlled, or operated by Yahoo, an email provider headquartered at 701 First Avenue, Sunnyvale, CA 94089; and

E. The Comcast Cable Communications ("Comcast") email address **debbiemiles@comcast.net** which is stored at premises owned, maintained, controlled, or operated by Comcast, an email provider headquartered at 650 Centerton Road, Moorestown, NJ 08057.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require:

- A. Microsoft to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the Microsoft email address **twshawdc@hotmail.com**.
- B. AOL to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the AOL email addresses **tcbgroupinc@aol.com**, **jimmendez320@aol.com** and **lauretteshaw@aol.com**.
- C. Google to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the Google email addresses **jshaw405@gmail.com**, **rrhame@gmail.com**, **terry.tcbgroup@gmail.com**, **thetgetteammanagers@gmail.com**, **SCGCompliance@gmail.com**, and **411webmarketing@gmail.com**.
- D. Yahoo! to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the Yahoo email addresses **dansilverman@yahoo.com** and **hectorperezpr@yahoo.com**.

E. Comcast to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the Comcast email address **debbiemiles@comcast.net**.

including, for Microsoft, AOL, Google, Yahoo!, and Comcast, the contents of communications.

3. I am employed as a Special Agent with the FBI in Atlanta, Georgia. I have been employed as a FBI agent since April 2003. I am currently assigned to the Atlanta Field Office Complex Financial Crimes squad. My current duties include the full-time investigation of financial crimes including wire fraud and money laundering. Moreover, I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7). As such, I am empowered to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. §§ 1343 (wire fraud) and 1956 (money laundering), and for other federal felony offenses. Prior to my employment with the FBI, I worked for approximately 5 years in the accounting industry, part of which as a Certified Public Accountant. My training includes attending the FBI Special Agent Training Program at the FBI Academy in Quantico, Virginia, a course designed to train new FBI agents in criminal law and investigative techniques.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information I obtained from various law enforcement agents, to include FBI Cyber Crimes Squad agents, and others. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included in this affidavit every detail of every aspect of the investigation. Rather, I have set forth facts that I believe are sufficient to establish probable cause for the issuance of the requested search warrant. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.



INVESTIGATION INTO STERLING CURRENCY GROUP

5. As detailed in this affidavit and the affidavit of Special Agent Roderick Coffin, which was submitted in application of additional email search warrants (see "Attachment C" for warrant, application, and accompanying affidavit for various Gmail accounts), the U.S. Attorney's Office for the Northern District of Georgia, the FBI, and the Internal Revenue Service (IRS) have initiated an investigation into Sterling Currency Group ("Sterling"), an Atlanta-based currency exchanger, for its suspected involvement in making false statements about the Iraqi dinar in order to increase sales. I believe that Sterling employees and/or contractors as well as other individuals linked to Sterling used interstate wires, including the registration and operation of websites, sending emails, and speaking on the telephone with customers, in furtherance of a scheme to defraud Iraqi dinar investors.

6. Sterling – which is also known as DinarBanker - is a currency dealer located in Atlanta, Georgia that specializes in the sale of Iraqi dinars and other types of currencies, such as the Vietnamese dong, the Indonesian Rupiah, the Afghani, and the Chinese Yuan. Financial records obtained during the investigation revealed that Sterling has obtained hundreds of millions of dollars from customers through dinar sales. Many individuals in the United States purchase Iraqi dinars in hopes that the dinar will "revalue" or gain in price compared to the U.S. dollar. Several states and a consumer protection group have warned that this is a risky investment and is likely a scam.

7. The investigation has revealed that Sterling has made a variety of false statements over the internet and telephone to induce customers to purchase the dinar. Sterling's website in 2010 promoted the dinar as a good investment. Sterling's website in 2010 also falsely claimed that if a currency "revaluation" occurred, customers would be able to exchange their dinars for

U.S. currency at airports all over the country. A Sterling employee falsely told a customer over the telephone that airport kiosks would be available following a revaluation. Furthermore, Sterling Chief Operating Officer Frank Bell and Sterling Information Technology contractor Youssef Hodaigui created anonymous blogs in 2012 that made false statements about the dinar. A former Sterling employee has confirmed to investigators that Sterling employees used anonymous blogs to make false claims about the dinar and direct prospective clients to Sterling.

8. On January 22, 2015, United States Magistrate Judge Russell G. Vineyard authorized search warrants of a variety of email addresses related to this case, including shawmarket@aol.com, which is believed to have been used by Sterling co-owner and co-founder James Shaw, trhame@earthlink.net, tyrhame@earthlink.net, and trhameb@earthlink.net, which are believed to have been used by Sterling co-owner and co-founder Tyson Rhame, and franksterlingcurrencygroup@gmail.com, which is believed to have been used by Sterling Chief Operating Officer Frank Bell. (See "Attachment C" for Gmail materials). Investigators have begun to review the contents of these particular email accounts.

9. While the review of these email accounts is not yet complete, I have seen various emails that further suggest that several Sterling employees were knowingly involved in a scheme to defraud Iraqi dinar purchasers.

10. For example, on November 3, 2010, an email was sent from shawmarket@aol.com to trhame@earthlink.net. The email has the subject line, "Discussion Point," is addressed to "Ty" and the name "Jim" is written at the bottom. The writer of the email expresses his and "Laurette's" concerns regarding the legality of selling Iraqi Dinar. Carole Laurette Shaw is James Shaw's wife and, as indicated below, has been involved in Sterling operations. In this email, "Jim" wrote, in part, "[s]he has lately been very nervous and

was crying last night because she knows we are running an illegal operation. The point is that her and I have worked way too hard in life for us to risk everything based on your belief (even if I agree with you) that the Iraqi dinar will not RV and it is ok to make millions of dollars in false promises to our customers. Not only are we risking everything we own, we are risking serious jail time as promoters of a ponzi scheme.” A copy of this email is attached to this affidavit as “Attachment D.” This email was sent in late 2010. Records obtained from North Dade Community Bank included a 2011 tax return for Sterling Currency Group that indicated Sterling reported \$245,411,774 in gross receipts or sales in 2011.

11. As referenced in the attached affidavit, Cooperating Witness 1 (CW1) is a former Sterling employee who has informed law enforcement that he was fired once he told Sterling employees to stop making comments on anonymous Iraqi dinar blogs. In an email from franksterlingcurrencygroup@gmail.com on behalf of frank@sterlingcurrencygroup.com sent to shawmarket@aol.com and trhame@earthlink.net titled “SEO Audit Cover,” and dated July 10, 2012, James Shaw expresses his desire to continue to utilize the website dinarbanker.com as the company’s primary website. The email contains what appeared to be an email thread between an individual named “Cyrus Shepard” and “Frank Bell.” In one exchange, “Frank Bell” writes a list of items that “Youseff is now doing based on Cyrus’ recos.” Number 2 on the list states, “SEOed blogs with “paid” ads for SCG/DB on them one is on page one ([First name of Cooperating Witness 1] unilaterally had Roberta pull down 3 of the 4 we had on page one telling her she could go to jail if she did not, I just found this out yesterday).” The email exchange is signed “Frank Bell Chief Operating Officer.” I believe that this corroborates the statement of CW1 that CW1 did in fact warn Sterling employees to not operate or otherwise utilize the anonymous blogs.

12. On August 6, 2012, an email containing a link to a Forbes Article was sent from shawmarket@aol.com to frank@sterlingcurrencygroup.com, with the subject line “not great article.” The title of the article is “You Can’t Fix Stupid: The Iraqi Dinar Scam Lives.” The link to the Forbes article was also sent from shawmarket@aol.com to trhame@earthlink.net on August 6, 2012 without a subject line. A search on the internet for an article with this name revealed a Forbes article that went into great detail describing how the sale of Iraqi Dinar is a scam and provided thoughts on why the dinar will never revalue.

13. I believe that these emails provide further evidence that Sterling employees, agents, affiliates, and/or contractors are knowingly engaged in a scheme to defraud dinar investors.

ADDITIONAL EMAILS TO BE SEARCHED

14. The investigation to date has revealed that several additional emails were used to conduct Sterling business, promote the Iraqi dinar, or otherwise facilitate the sale of dinars and other currencies, and likely have relevant evidence, including but not limited to, information pertaining to Sterling’s operations, the identities of Sterling’s customers, the sale of Iraqi dinars, communications with regulators, communications with financial institutions, the states of mind of these individuals, and the disposition of proceeds.

**Jshaw405@gmail.com – Alternative James Shaw Email Address**

15. I believe that **jshaw405@gmail.com** is an alternative email address of Sterling co-founder and co-owner James Shaw.

16. On an Arkansas Money Services Application for Sterling Currency Group dated February 9, 2011, and signed by “James S Shaw,” Shaw’s email address is listed as **jshaw405@gmail.com**. On February 10, 2011, shawmarket@aol.com forwarded an email to

**jshaw405@gmail.com** that stated, "Fwd: Sterling Currency Group AML and Independent audit." On March 29, 2011, a bank official sent an email to "Ty Rhame" and **jshaw405@gmail.com**." The subject of the email was "Sterling Currency Group." The email dealt with Sterling's application to open an account at this particular bank.

**Lauretteshaw@aol.com – Carol Laurette Shaw**

17. I believe that **lauretteshaw@aol.com** is being used by Carol Laurette Shaw, James Shaw's wife and one-time employee of Sterling.

18. Mercantile records show that a document was at one point sent to Mercantile Bank from Sterling entitled "Sterling Currency Contact List. Laurette Shaw is listed twice on this list, including under a field titled, "Main Operational Contacts." Laurette Shaw's email address is listed as **lauretteshaw@aol.com**.

19. The email in which **shawmarket@aol.com** (believed to be James Shaw) describes this as a "ponzi scheme," was forwarded to **lauretteshaw@aol.com** on November 3, 2010. On August 11, 2011, an individual using email address **susan.sherman10@gmail.com** sent an email to **trhameb@earthlink.net**, **frank@dinarbanker.com**, and **lauretteshaw@aol.com**. The email was entitled "Update Tracking of 105 FinCEN Forms."

20. On December 23, 2014, **lauretteshaw@aol.com** sent an email to **frank@sterlingcurrencygroup.com** that stated, "[h]i Frank, Just making sure that someone is taking care of James Mendez this Christmas. I was just thinking about him today and didn't want to forget to check with you on it. Thanks, Laurette." The email is signed "Laurette Shaw, **lauretteshaw@aol.com**." After **frank@sterlingcurrencygroup.com** responded, **lauretteshaw@aol.com** wrote an email to **frank@sterlingcurrencygroup.com** on December 24, 2014, that stated, "in the past years we have always sent him a gift certificate to the ritz

carolton in san juan to il mulino.(300.00 I think) I'm not sure what they did last year or how much business he is doing this year." As referenced below, James Mendez is the operator of Mendez Internet Management Services, an Iraqi dinar exchanger in Puerto Rico, was at one point listed as an agent of Sterling, and has obtained millions of dollars' worth of dinar from Sterling.

**Jimmendez320@aol.com, Mendezinternet@gmail.com, Hectorperezpr@yahoo.com -- Mendez Internet Management Services**

21. I believe that **jimmendez320@aol.com, mendezinternet@gmail.com, and hectorperezpr@yahoo.com** are being used by individuals associated with "Mendez Internet Management Services," ("Mendez Internet") a company linked to Sterling that sells dinars in Puerto Rico.

22. Mendez Internet operates through the website <http://dinarespr.com/site/web/>, which is primarily written in Spanish. Mendez Internet is operated by an individual named James Mendez. Mendez appeared on a Puerto Rico news station in October 2014 to discuss his dinar business. A Spanish-speaking FBI language analyst has listened to this interview. During the interview, Mendez made various claims about the dinar, including: that the individuals who had invested in the dinar would be rich one day, that he had sold dinars to more than 400,000 customers, that reputable businessmen were investing in the dinar, that one investor-family purchased \$1 million worth of dinars, and that the federal government had looked into him and said everything was fine.

23. In a February 10, 2011, email, trhame@earthlink.net sent a copy of a Sterling Currency Group Bank Secrecy Act / Anti-Money Laundering Compliance review dated June 23, 2010. The report states Mendez Internet Management Services, Inc. was an agent of Sterling. A letter from Tyson Rhame that accompanied this report contains an "MSB Agent

List.” The only agent listed is “JAMES MENDEZ: (Operates Mendez Internet Management Services – a registered MSB).” In a January 7, 2015, email from [teresa@sterlingcurrencygroup.com](mailto:teresa@sterlingcurrencygroup.com) to an employee of the West Virginia Division of Banking that CC’d [frank@sterlingcurrencygroup.com](mailto:frank@sterlingcurrencygroup.com), the writer stated that, “as of 31 December 2014, Sterling Currency Group LLC continues to have no agents or delegates.”

24. However, the investigation has revealed that even if Mendez is not currently an official agent of Sterling, he has continued to purchase millions of dollars’ worth of Iraqi dinars and other currencies from Sterling and sell them to his own customer base. A January 7, 2015, email sent from a Sterling employee to [frank@sterlingcurrencygroup.com](mailto:frank@sterlingcurrencygroup.com) is entitled “Mendez 2014” balance, and states that, “[t]he attached contains an itemization of 2014 transactions.” Attached to this email is an excel sheet which lists a variety of orders and payments. The 2014 payments total over two million dollars.

25. On June 12, 2014, [jimmendez320@aol.com](mailto:jimmendez320@aol.com), responding to a prior email sent from [michael@sterlingcurrencygroup.com](mailto:michael@sterlingcurrencygroup.com) sent an email to [michael@sterlingcurrencygroup.com](mailto:michael@sterlingcurrencygroup.com), [frank@sterlingcurrencygroup.com](mailto:frank@sterlingcurrencygroup.com), and CC’d [hectorperezpr@yahoo.com](mailto:hectorperezpr@yahoo.com) and [trhame@earthlink.net](mailto:trhame@earthlink.net) that stated, “Got another payment going out today with approximately \$100k and a bit more. Will be there in the morning. Frank. Per your instructions I’m bringing down the payment ASAP. If Dongs come in, would appreciate an approval for an authorization. Thank you, **James Mendez.**”

26. [Jimmendez320@aol.com](mailto:jimmendez320@aol.com) sent an email to [frank@sterlingcurrencygroup.com](mailto:frank@sterlingcurrencygroup.com) and [trhame@earthlink.net](mailto:trhame@earthlink.net) on June 3, 2014, that stated, “Hi Ty and Frank, Have a contract here to purchase a large amount of dinars. Would like you to take a look at it and see if it is feasible? I haven’t done anything. Your thoughts please? Thanks, **James Mendez.**”

27. On January 14, 2015, **jimmendez320@aol.com** sent an email to **michael@sterlingcurrencygroup.com**, **frank@sterlingcurrencygroup.com**, and **hectorperezpr@yahoo.com** with the subject, "Revised price list." The email states, "Hi Michael, Hope all is well! Just to ask if you have a revised price list available starting for 2015?" The email is signed, "Thanks, **James Mendez**."

28. On January 16, 2015, **hectorperezpr@yahoo.com** sent an email to **catherine@sterlingcurrencygroup.com** and **frank@sterlingcurrencygroup.com**. The email CC'd **mendezinternet@gmail.com**. The subject of the email was "Mendez Internet Management Services Inc. 4<sup>th</sup> Quarter ComplianceReport." and the email was signed by:

Hector R. Perez  
Compliance Officer  
Mendez Internet Management Services Inc.

The email attached a document entitled "Sterling Report (October to December 2014). The attached document states at the top "Mendez Internet Management Services, Inc." and states, "[a]s per request of *Sterling Currency Group* Compliance Program, we send you the following information for the fourth quarter of 2014:" The email then lists various transactions. For instance, a chart indicates that there were a total number of 845 transactions regarding the Iraqi dinar from October to December 2014. The bottom of the document states in part, "[m]y email is **hectorperezpr@yahoo.com** and our phone numbers are . . . ." and is signed by "Hector R. Perez."

**twshawdc@hotmail.com – Terry Shaw**

29. I believe that **twshawdc@hotmail.com** is being used by Terry Shaw, who is James Shaw's relative, a potential purchaser of Iraqi dinars, and who appears to have assisted Sterling establish a banking relationship with Mercantile Bank in Quincy, Illinois.



30. I have reviewed several emails in which shawmarket@aol.com communicates with twshawdc@hotmail.com. In an email dated November 19, 2010, twshawdc@hotmail.com wrote to shawmarket@aol.com, "Jim: Tracy was contacted by a friend who is has heard that, with a new PM, Iraq's denar is going to skyrocket. Tracy is interested but I told her I would contact you to get your opinion. Do you think there is going to be a big jump in the value of the denar in the near future based on political changes and based on their oil reserves etc.? Would you recommend buying now or is this just a huge crapshoot now and in the future? What is the cost to buy from you?" The email is signed "Terry W. Shaw" and indicates that the writer is a licensed acupuncturist in Quincy, Illinois. From reading other emails, I believe that Terry and Jim Shaw are related to one another. On November 20, 2010, shawmarket@aol.com wrote to twshawdc@hotmail.com, "Terry, These rumors have been around for a while but nothing major has happened. With that said, our business is out of control as we have just added many full-time employees. I think the currency will go up in value in a slower less dramatic way than the rumor mills predict. (www.dinarbanker.com) Without telling Tracy, who we are, ask her where she was referred to buy dinar from? We are second largest in US but have been making ground up as we now have the bloggers singing our praises. Almost a little cult like." The email is signed "Jim."

31. On January 20, 2011, twshawdc@hotmail.com sent an email to shawmarket@aol.com entitled "Dinar" that stated, "How many Dinar can you get me for \$2,500.00? Seems like there is more and more talk of the Dinar being revalued." On January 21, 2011, shawmarket@aol.com wrote an email to twshawdc@hotmail.com that stated, "Send me the money. Maybe around 2.3-2.6 million. We now have 10 full time employees plus a 17 person call center". On January 21, 2011, shawmarket@aol.com wrote an additional email to

**twshawdc@hotmail.com** that stated in part, "business is great but this is the weirdest increidbily successful venture I could ever have imagined. I will sell it to you at a slightly higher price if you want to flip it other Quincyans and we could both make profit on sale."

32. In a March 15, 2011, email shawmarket@aol.com wrote to **twshawdc@hotmail.com** that "Banking is a big problem for Sterling Currency even though were willing to pay 40-50K per month in fees. Is there a Quicny bank who you have huge clout with and is somewhat modern. Well pay a finders fee as were running out of options for our dinar business. Banks are hugely afraid of money service businesses because of alll the compliance. Nothing new on the dinar front as of yet." The investigation has determined that at one point Sterling had accounts open at Mercantile Bank, a bank located in Quincy, Illinois. On July 12, 2011, shawmarket@aol.com wrote to **twshawdc@hotmail.com** that, "If you have another bank now is the time. It looks like FDIC is telling Mercantile to close our account immediately and they have no reason at all. Ted and Shari are furious but it looks imminent. Time is of the essence even though our agreement was for 60 days. I am back from Europe tomorrow."

**Rrhame@gmail.com – Rhett Rhame**

33. I believe that **rrhame@gmail.com** is being used by Rhett Rhame, who is Tyson Rhame's brother and Sterling employee.

34. As referenced in the attached affidavit, former Sterling employee CW1 (described in the attached affidavit) had overheard Rhett Rhame falsely tell a customer over the telephone that following a revaluation, Sterling would set up kiosks at major airports. On January 15, 2012, an email was sent from "Rhett Rhame" to "Ty Rhame" entitled, "Thank You." The email stated, in part, "I hesitate to bring up the part about not feeling of much value at Sterling, but I

have been feeling this way for quite some time now. That is just part of my personality and character to want to feel more involved and valued. But by the same token, I do not want to be perceived just being there because I am your brother. I downplay being your brother every chance I get - even though I am so incredibly proud of everything you (& Tripp) have done and become! And I say that genuinely with great pride and joy."

35. In response to this email, "Ty Rhame," using trhame@earthlink.net sent an email to "Rhett Rhame" at rrhame@gmail.com on January 16, 2012, that stated, in part, "As far as office communications go, that needs to be addressed and more information needs to be shared regarding policies. I'm normally hesitant to say or share too much with anyone in the office because of the potential harmful consequences--even Frank is left out of many discussions and issues. I'm glad you shared that you 'get it' regarding sharing information. By a long shot, you are not the only one that has made that mistake. That mistake has been made by several people in the office and yours was minor compared to some others. Frank cost us 30K while we were at the beach because of something he shared with the wrong people. It took a lot of time and experience for me to get to the point where I carefully consider everything before it comes out of my mouth or I write in an email. I've learned that people will often twist, interpret, or relay information in a way I never intended, if I'm not very very careful. In our business with our internet and forum exposure, one misstep can cause a lot of headache, lawsuit, or expense. Anyway, you get it and I won't worry about you having any issues with that in the future. Slipups do happen, and we can only learn from them."

**tcbgroupinc@aol.com, terry.tcbgroup@gmail.com, thegetteammanagers@gmail.com – TCB Group / The Get Team**

36. I believe that **tcbgroupinc@aol.com**, **terry.tcbgroup@gmail.com**, and **thegetteammanagers@gmail.com** are used by the operators of "The Get Team" website, which is a website that discusses that Iraqi dinar and on which Sterling advertises.

37. The investigation has determined that Sterling advertises on a variety of websites that discuss the Iraqi dinar. One of these websites is <http://thegetteam.com/>.

38. The About Us Section of thegetteam.com states, among other things:

- We are the largest Dinar Website
- Latest News and Updates on the Iraqi Dinar
- Great Round Table Conference Calls
- Best Dinar Dealers in Chat and on our call to answer your questions; and
- Free Site, Free Chat, Free Forum

The About Us section also states, "On behalf of TerryK, Gankans and Support Team, we want to welcome all of you – old and new – to your new home!" Law enforcement has not yet accessed the chat room of this particular website as one needs to become a member to gain access to this part of the website. However, I have conducted research on the Internet for "TerryK dinar." On the website "dinarrecaps.com" I viewed what appears to be saved postings from "TerryK." This particular website states, in part, that, "[w]e monitor multiple chat rooms, forums and websites for the very best Iraqi Dinar information and quotes from the Dinar 'Guru's'. With the help of other forums and chat rooms, we will bring conference call times and access codes to our followers." One link stated, "Terryk And Get Members Chat Thursday Afternoon" and is dated "1/3/2013." The following information was posted:

[TERRYK] WELL FIRST OF ALL DKG THE DONG IS GOING WITH THE  
DINAR. ITS ONE OF THE PRIMARY 11 CURRENCIES IN THE BASKET.

PERIOD. SO THAT TELLS YOU WHAT THEY KNOW. SECOND THERE ARE 194 COUNTRIES THAT ARE INVOLVED IN THIS ECONOMIC RESET THATS ABOUT TO TAKE PLACE

[BamaSteve] TERRYK Is this afternoon still a strong possibility?

[TERRYK] BAMA WHY ARE U ASKING THAT, AND TO ANSWER YOU YES . RUMOR IS 4PM EST IS VERY STRONG

[BamaSteve] TERRYK You had said the 3rd around bank closing time.

[TERRYK] GETTING THAT FROM A COUPLE OF SOURCES. NOW I JUST DONT KNOW IF 4 PM EST IS THE RIGHT TIME AS IT WOULD NOT BE FAIR TO DO THAT WITH THE BANKS CLOSED ON THE EAST COAST AND THEM OPEN ON THE WEST. BUT THATS THE RUMOR

[BamaSteve] Is there a time globally when all banks are closed?

[TERRYK] 2-3 AM BAMA IS WHAT I HAVE BEEN TOLD THAT ALL THE BANKS TALK

[kellee] TERRYK I am new to allof this. "If" they RV today, about how long do we wait to cash in. I am not sure long long go through the roof is

[TERRYK] KELLEEE I CANT TELL YOU THAT, BUT FOR ME NO MATTER WHAT IT COMES OUT AT IM CASHING A MIL OR TWO IN, AND WATCHING

[TERRYK] OK, HERE IS WHAT I GOT AND ITS HOT. TONIGHT IS RED HOT. RED HOT. HAVE ANOTHER CALL COMING IN SOON TO GIVE ME MORE DETAILS. PP ARE OUT BEING DELIVERED. HAVE 3 CONFIRMS

ON THAT. WE ARE IN THE MONEY PEEPS. WHOO HOO. TREAT AS  
RUMOR OF COURSE

While this information did not come from directly from <http://thegetteam.com/>, it is representative of the type of material that I am aware exists within the dinar investor community.

39. Financial records reviewed during the investigation reveal what appear to be \$4,000 monthly payments from Sterling to "TCB Group, Inc." located at 504 Sherwood Drive in Grayson, Kentucky 41143. A search of the Kentucky Secretary of State website revealed a company in active status named "TCB Group Inc." located at the above-listed address. The Certificate of Authority for TCB Group states that the entity's representatives are "Susan C Keller" and "Terrence Lynn Keller." Based upon the above and my knowledge of the case, I believe that TerryK is Terrence Lynn Keller.

40. A September 13, 2010, email to "Ty Rhame," from [tcbgroupinc@aol.com](mailto:tcbgroupinc@aol.com) contains the subject line, "RE: [www.thegetteam.com](http://www.thegetteam.com) dinar conference call." The email states, "Ty, My name is TerryK, I own the worlds largest Dinar web site going....we have currently 7200 members and currently we hold two calls a week with about 1500 on the call and 100's if not 1,000's on skype listening in...what I would like to do is open a discussion with you and maybe have you on a call this coming wed night. It starts at 9pm and thought maybe 10-15 min on how you operate, how to cash in with your firm and then a question and answers session....let me know via email ." The email is signed "terryk".

41. On August 6, 2014, [thegetteammangers@gmail.com](mailto:thegetteammangers@gmail.com) sent an email to several individuals, including [frank@sterlingcurrencygroup.com](mailto:frank@sterlingcurrencygroup.com) and [terry.tcbgroup@gmail.com](mailto:terry.tcbgroup@gmail.com) that provided a conference call number, host access code, and participant code. The email was signed "-tina".

42. On September 29, 2014, **terry.tcbgroup@gmail.com** sent an email that CC'd **frank@sterlingcurrencygroup.com** with the subject line, "Reserve." The email stated, "Frank, looking to do a 30 day layaway, sending you thru another person that owes me money 10 – 15k what type of layaway \$\$\$\$ wise can I get." The email is signed, "TK."

43. On November 5, 2014, email from **terry.tcbgroup@gmail.com** to **frank@sterlingcurrencygroup.com** has the subject "Price on Dinar." The email states, in part, "Frank, I need pricing on the following on what I have given away and in addition to what we are giving away for our donation drawing currently going on....Please price out the following for me...." The email then contains different currency amounts such as "50 dinar notes ( 3 bundles ) = 100 notes per bundle," "(250 dinar notes (3 bundles ) = 100 notes per bundle," and "5 million dong 20k notes." The email is signed,

Thanks buddy

Terrence (Terry) Keller  
CEO TCB Group Inc  
606-474-9257 O  
205-568-3600 C  
**terry.tcbgroup@gmail.com**

44. A November 12, 2014, email from **terry.tcbgroup@gmail.com** to **thegetteammanagers@gmail.com** states, in part, "Please cut a check from tcb caring hands for 690.00 to Sterling Currency Reference this order number and the name Terrence Keller **ORDER #9128552.**" The email is signed

Terrence (Terry) Keller  
CEO TCB Group Inc  
606-474-9257 O  
205-568-3600 C  
**terry.tcbgroup@gmail.com**

The email address **thegetteammanagers@gmail.com** then forwarded this email to **frank@sterlingcurrencygroup.com** and stated, "Frank, Can I do an e-check for this order or do you want me to mail it?" The email was signed, "Tina."

**Debbiemiles@comcast.net – IQD Team Connection Account**

45. I believe that **Debbiemiles@comcast.net** is used by an operator of "The IQD Team Connection" website, which is an additional website that discusses the Iraqi dinar and on which Sterling advertises.

46. "The IQD Team Connection" is located at <http://www.theiqdteamconnection.com/>. The website contains a variety of internal links. One of the links is "PRE & POST RV Information." The website also references a conference call number.

47. On November 12, 2014, an email was sent from **debbiemiles@comcast.net** to **frank@sterlingcurrencygroup.com** with the subject "Hi Frank" that stated, in part:

Hope all is well...  
Could you please check on our check for the month of November  
We have not received yet.

Also I wanted to ask you about XA and Dinar Trade – some comments made on a post about their new locations

The email is listed as being from "Debbie Miles" at "The IQD Team Connection."

48. On January 15, 2015, **debbiemiles@comcast.net** sent an email to **frank@sterlingcurrencygroup.com** with the subject, "\$24 million Iraqi dinar currency scam." The email contains a link to a CNBC video regarding a recent case in the Northern District of Ohio in which individuals were sentenced for participating in a scheme to defraud investors of the Iraqi Dinar and hedge funds. The email also stated:

**In case you haven't seen this...**



**Smiles**

**Deb**

49. Records from Mahopac Bank indicate that Sterling has made what appear to be monthly payments in the amount of \$3,000 to "Granite Rock TCI, LLC." Several of the checks to "Granite Rock TCI, LLC" state, "dba The I.Q.D. Team Connection."

**411webmarketing@gmail.com – Additional Youssef Hodaigui Account**

50. I believe that **411webmarketing@gmail.com** is used by Sterling IT contractor Youssef Hodaigui.

51. As referenced in the attached affidavit signed by Special Agent Coffin, Youssef Hodaigui is a Sterling IT contractor. On January 23, 2014, **411webmarketing@gmail.com** sent an email to **trhame@earthlink.net** and **trhameb@earthlink.net** (both believed to be Tyson Rhame) that contained the username **ty@sterlingcurrencygroup.com** and a password. The email was signed, "Regards, Youssef Hodaigui." On March 21, 2014, **411webmarketing@gmail.com** sent an email to **trhame@earthlink.net** (believed to be Tyson Rhame) that stated, "Your mailbox **ty@scg** compromised. Here is the new password." The email states in part, "Ty, your mailbox **ty@sterlingcurrencygroup.com** password has been compromised. I changed your password to . . . ." The email is signed "Regards, Youssef Hodaigui."

**Dansilverman@yahoo.com – Dan Silverman Account**

52. I believe that **dansilverman@yahoo.com** is used by the one-time owner of GID Associates, an Iraqi dinar exchanger that was purchased by Sterling in 2013.

53. Sterling is not the only currency exchanger that sells Iraqi dinars in the United States. For several years, GID Associates was a Sterling competitor. A 2010 report of

Independent Examination regarding the Bank Secrecy Act / Anti-Money Laundering Compliance states that GID Associates was created to sell Iraqi dinars to the domestic market and was operated by an individual named "Dan Silverman" in Connecticut. Records from Actors Federal Credit Union indicate that Sterling acquired GID Associates in 2013. Chelsea Bank records revealed an email from frank@sterlingcurrencygroup.com that stated, in part, "[a]s I mentioned last week, we have purchased a competitor and are integrating their operations into our. The purchase was an asset purchase, and we intend to continue to operate the company under the brand name of the old company, "GID Associates".

54. A May 16, 2014, email from dansilverman@yahoo.com to frank@sterlingcurrencygroup.com and trhame@earthlink.net states, in part:

<https://www.google.com/#q=sterling+currency+group+gid+associates>

I did a google search for the two domains. d/b/a/ filings could have triggered Robert's fishing expedition

I also see that Ali changed his site and dropped price

Please keep me informed of anything else that comes up and I will do the same

Now four months later, and New Year, and I have not been following any dinar trends/sites/chats, etc.

I hope 2014 remains a good year for you and companies

Best,

Dan

55. A May 16, 2014, email from dansilverman@yahoo.com to frank@sterlingcurrencygroup.com and trhame@earthlink.net with the subject line, "Title 31 audit not needed," states, in part, "Apparently an IRS agent called the toll free number and SCG

told him SCG purchased the assets of GID and referred to my cell". The email was signed "Dan."

**SCGCompliance@gmail.com – Catherine Rualo Thomas / Sterling Anti-Money Laundering Compliance Account**

56. I believe that SCGCompliance@gmail.com is used by Sterling Anti-Money Laundering / Bank Secrecy Act ("BSA/AML") compliance personnel.

57. The investigation has revealed that an individual named Catherine Rualo Thomas is the Chief AML/BSA Compliance Officer for Sterling. Rualo Thomas is listed as the Chief Compliance officer on various documents submitted to banks and other entities. On November 5, 2014, "Catherine Thomas," using catherine@sterlingcurrencygroup.com sent an email to frank@sterlingcurrencygroup.com with the subject, "Logins for Gmail & Dropbox." The email contained, in part, the following information:

Gmail:

**SCGCompliance@gmail.com**

Password: 3277RoswellRoadNE

The password is the official Sterling mailing address in Atlanta, GA. The email is signed "Catherine R. Thomas (formerly Rualo)," as the "Chief Compliance Officer" for "Sterling Currency Group."

**GOOGLE RECORDS**

58. Based on my training and experience as well as information I have obtained from the FBI Cyber Crimes Squad, I have learned that Google, Inc. ("Google") provides a variety of on-line services, including electronic mail ("email") access, to the general public. Google allows subscribers to obtain email accounts at names chosen by the subscriber, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the

registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information.

59. In general, an email that is sent to an Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

60. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google server, the email can remain on the system indefinitely. Even if the sender deletes the email, it may continue to be available on Google's servers for a certain period of time.

61. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by Google but may not include all of these categories of data.

62. Subscribers to Google might not store on their home computers copies of the emails stored in their Google account. This is particularly true when they access their Google

account through the web, or if they do not wish to maintain particular emails or files in their residence.

63. In general, email providers like Google ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

64. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

65. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

66. Based on my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

67. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require:

- a. Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

68. Based on the forgoing, I request that the Court issue the proposed search warrant.

69. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

70. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

**ATTACHMENT A**

**Property to Be Searched**

1. This warrant applies to information associated with the email addresses **jshaw405@gmail.com, rrhame@gmail.com, terry.tcbgroup@gmail.com, thegetteammanagers@gmail.com, SCGCompliance@gmail.com, and 411webmarketing@gmail.com** which are stored at premises owned, maintained, controlled, or operated by Google, Inc., an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google, Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

A. The contents of all emails stored in the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

B. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

C. All records pertaining to communications between Google, Inc. and any person regarding the account, including contacts with support services and records of actions taken.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 1343 and 1956 and conspiracy to commit these



offenses, including for each account or identifier listed on Attachment A, information pertaining to the following matters:

- A. The identity of the person(s) who created, used, or communicated with the account or identifier, including records that help reveal the whereabouts of such person(s).
- B. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events.
- C. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation.
- D. Records relating to buying and selling of currency, commodities, and securities.
- E. Records related to the users' financial information, including but not limited to bank accounts, tax information, additional sources of income or revenue, expenditures, and the disposition of proceeds.
- F. Records relating to Sterling Currency Group / DinarBanker, including but not limited to the corporate structure, correspondence with Sterling employees, payments from Sterling, direction from Sterling employees, and corporate documents.
- G. Records relating to websites that discuss currency sales or exchanges, including but not limited to, registration and maintenance of the websites, statements on the websites, and payment information.
- H. Records related to the advertisement of Sterling Currency Group / DinarBanker.
- I. Records related to the users' involvement with web development, web design, and blog registration or maintenance.

DUPLICATE

(Rev. 4/30/2014) Search Warrant

## United States District Court

Northern District of Georgia

In the Matter of the Search of:

Information associated with the email addresses  
 Franksterlingcurrencygroup@gmail.com,  
 uyopilot@gmail.com, denamanzo@gmail.com that is stored  
 at premises owned, maintained, controlled, or operated by  
 Google, Inc., an email provider headquartered at 1600  
 Amphitheater Pkwy, Mountain View, CA 94043

## SEARCH WARRANT

CASE NUMBER: 1:15-MC-37

UNDER SEAL

TO: FBI Special Agent Roderick F. Coffin and any Authorized Officer of the United States:

An affidavit having been made before me by Special Agent Roderick F. Coffin, who has reason to believe that, on the property or  
 premises known as

See Attachment A

There is now concealed certain property, certain data, and certain information, namely,

See Attachment B

which constitutes evidence of the commission of a criminal offense and property which has been used as the means of committing a  
 criminal offense, concerning violations of Title 18, United States Code, Sections 1343 and 1956, over which the United States District  
 Court for the Northern District of Georgia has jurisdiction. I find that the affidavit establishes probable cause to search and seize the  
 person or property from the person or premises described above.

YOU ARE HEREBY COMMANDED to execute this warrant on or before 2/5/15  
 Date

(not to exceed 14 days) AT ANY TIME IN THE DAY OR NIGHT AS I FIND GOOD CAUSE HAS BEEN ESTABLISHED. You must  
 give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was  
 taken, or leave a copy of the warrant and receipt at the place where the property was taken. The officer executing the warrant, or an  
 officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant  
 and inventory to United States Magistrate Judge Russell G. Vineyard

January 22, 2015 at 11:54 am  
 Date and Time

at Atlanta, Georgia  
 City and State

RUSSELL G. VINEYARD  
 UNITED STATES MAGISTRATE JUDGE  
 Name and Title of Judicial Officer

Russell G. Vineyard  
 Signature of Judicial Officer

AUSA Thomas J. Krepp / 404-581-4647

GOVERNMENT  
EXHIBIT

C

SW-000190

**ATTACHMENT A**

**Property to Be Searched**

1. This warrant applies to information associated with the email addresses **youssefhodaigui@gmail.com**, **franksterlingcurrencygroup@gmail.com**, **uyopilot@gmail.com**, and **denamanzo@gmail.com** which are stored at premises owned, maintained, controlled, or operated by Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.